TITLE:

Kolyvaginによる楕円曲線のTate-Safarevic群についての仕事の紹介(代数的整数論)

AUTHOR(S):

栗原, 将人

CITATION:

栗原, 将人. Kolyvaginによる楕円曲線のTate-Safarevic群についての仕事の紹介(代数的整数論). 数理解析研究所講究録 1990, 721: 102-116

ISSUE DATE:

1990-05

URL:

http://hdl.handle.net/2433/101833

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
721巻 1990年 102-116

Kolyvaginによる楕円曲線のTate-Šafarevič群についての仕事の紹介

東京都立大理　栗原　将人（Masato Kurihara）

この稿はKolyvaginの最近の論文（preprint）"Euler systems"[1]の解説である。円分体（あるいは楕円曲線の等分点をつけ加えて得られた体）のideal類群、あるいは岩澤のMain Conjectureについてのの仕事については市村氏の解説に譲り、ここでは楕円曲線のTate Šafarevič群の有限性、あるいはその位数を押さえようという仕事についての紹介をしたいと思う。Kolyvaginの言うEuler systemという概念がいかにうまく働くかということをわかりやすく解説するために、ここでは[1]をRubin[3]風に解釈し直して話を進める。このときGross[5]も参考になる。ただし[1]は内容がかなり豊富であり、ここに述べるのはその主要部分だけであり、[1]のすべてを紹介するわけではないことを最初に断っておく。

Convention

Abel群Aに対して、n倍写像の核、余核をそれぞれ${}_nA$, A/nと書く。

§1. Birch Swinnerton-Dyer conjecture

ここでは有名な楕円曲線に関する Birch Swinnerton-Dyer 予想について復習する。K を代数体，E を K 上定義された楕円曲線とするとき，E/K の L 関数 $L(E/K, s)$ が定義される（たとえば cf [6], [7]）。$L(E/K, s)$ は $\mathrm{Re}(s) > \frac{3}{2}$ で正則である。

Conjecture. (Birch, Swinnerton-Dyer) $L(E/K, s)$ は全平面に解析接続され，

1) $L(E/K, s)$ の $s=1$ での零点の order は $\mathrm{rank}\, E(K)$ に等しい。

(Mordell Weil の定理により K 有理点の群 $E(K)$ は有限生成 abel 群，$\mathrm{rank}\, E(K)$ はその rank である。)

2) $L(E/K, s)$ の $s=1$ での零点の order を r とすると

$$\lim_{s \to 1} \frac{L(E/K, s)}{(s-1)^r} = \frac{\#Ш(E/K) \cdot \det \langle , \rangle}{(\#E(K)_{\mathrm{tors}})^2 \sqrt{|d_K|}} V_\infty V_{\mathrm{bad}}$$

ここに $Ш(E/K) := \ker\left(H^1(K, E) \to \prod_{v:\text{all primes}} H^1(K_v, E)\right)$ がこの話の主役 Tate Šafarevič 群，$\det \langle , \rangle$ は height pairing による regulator，V_∞ は E の無限素点の様子にしかよらない数 (period)，V_{bad} は E a bad reduction のところの様子にしかよらない数 $\left(= \prod_{v:\text{finite}} (E(K_v) : E^\circ(K_v))\right.$ ここに $E^\circ(K_v)$ は reduction が smooth な点全体$\left.\right)$，d_K は K の判別式である。

1) についてもたくさんの部分的結果があるが，ここでは焦点を 2) にしぼることにする。

Remark 1. K の Dedekind zeta $\zeta_K(s)$ の $s=1$ での leading term

$$\lim_{s\to 1}\frac{\zeta_K(s)}{(s-1)}=\frac{h_K\cdot R_K}{\#\mu(K)^2\sqrt{|d_K|}}\cdot 2^{r_1}\cdot(2\pi)^{r_2}$$

(h_K：類数、R_K：regulator) と比べると $\#Ш(E/K)$ が類数にあたっていることがわかる。

Remark 2. つい最近まで この予想が成立する楕円曲線の例は一本も知られていなかった。それは $Ш(E/K)$ が有限群となる例が一つも知られていなかったからである。ただし自然数 n に対して ${}_nШ(E/K)$ が有限であることは昔から知られており (cf. 11 ページ)、多くの例について計算されていた。

最初に $\#Ш(E/K)<\infty$ なる例を与えたのは Rubin である。彼は虚二次体 K 上定義された complex multiplication を持つ楕円曲線 E ($\mathrm{End}(E)\otimes\mathbb{Q}=K$) に対して $L(E/K,1)\neq 0$ であれば $Ш(E/K)$ は有限であることを示した ([4])。このとき key となったのは elliptic units の arithmetic と ideal 類群の annihilator を与える元を作る Kummer Thaine の idea (cf. [8], [3]) であった。Euler system はこの Kummer Thaine の idea の一般化である。Euler system の存在を使って このような E/K に対しては Birch Swinnerton-Dyer 予想をほぼ証明することができる。(Rubin が論文を準備中のようである。)

§2. Statement of the main results

E を $\mathbb{Q}$ 上定義された楕円曲線、modular curve で parametrize

されているとする。(Taniyama Weil 予想によれば $\mathbb{Q}$ 上の楕円曲線はすべてこの性質を持つ。) すなわち E の conductor を N_0 として

$$\varphi : X_0(N_0) \longrightarrow E$$

なる surjective morphism が存在するとする。

E は $\mathbb{Q}$ 上定義されているが、Gross Zagier の公式 (cf. 6ページ) が虚2次体上にあるために、E を虚2次体 K 上の楕円曲線と見て Birch Swinnerton-Dyer 予想を考える方が都合がよい。そこで $-D \equiv$ square $(\mathrm{mod}\ 4N_0)$, $(D, 2N_0)=1$ なる $D>0$ をとり判別式 $-D$ の虚2次体 $K=\mathbb{Q}(\sqrt{-D})$ を考える。このとき Kolyvagin は次を示した。

Theorem 1. $L'(E/K, 1) \neq 0$ であれば $Ш(E/K)$ は有限群、さらに $\mathrm{rank}\, E(K) = 1$.

Remark 1. 仮定から $L(E/K, 1) = 0$ であり上の仮定は $\mathrm{order}_{s=1} L(E/K, s) = 1$ と同じである。

Remark 2. 「$Ш(E/K)$ が有限」は「$Ш(E/\mathbb{Q})$ が有限」を導く。これは $n \cdot Ш(E/K) = 0$ が $2n \cdot Ш(E/\mathbb{Q}) = 0$ を導くことによる。

Remark 3. Gross Zagier の公式 (6ページ) により、$\mathrm{rank}\, E(K) \geq 1$ はすでにわかっていた。上により Birch Swinnerton-Dyer 予想 a 1) が $L'(E/K, 1) \neq 0$ の仮定の下確かめられたことになる。

Remark 4. Kolyvagin の前論文 [2] では $L'(E/K, 1) \neq 0$ の仮定の下, $L(E/\mathbb{Q}, s)$ の関数等式の符号が $+1$ のとき $Ш(E/\mathbb{Q})$ の有限性を示していた。Euler system を考えることにより, 関数等式の符号についての仮定は不必要になったのである。

$\mathbb{Q}$ 上の予想を上から導くには

$$L(E/K, s) = L(E/\mathbb{Q}, s) \cdot L(E/\mathbb{Q}, \chi, s)$$

を使えばよい。ここに χ は $K/\mathbb{Q}$ に対応する Dirichlet 指標。

Corollary 1. $\operatorname{order}_{s=1} L(E/\mathbb{Q}, s) = 1$ であれば $Ш(E/\mathbb{Q})$ は有限, さらに $\operatorname{rank} E(\mathbb{Q}) = 1$.

∵) Waldspurger の定理により $L(E/\mathbb{Q}, \chi, 1) \neq 0$ なる K がとれ, Th. 1 を適用できる。

Corollary 2. $L(E/\mathbb{Q}, 1) \neq 0$ であれば $Ш(E/\mathbb{Q})$ は有限, さらに $\operatorname{rank} E(\mathbb{Q}) = 0$ (つまり $E(\mathbb{Q})$ も有限群).

∵) 最近証明された analytic conjecture を使えば $\operatorname{order}_{s=1}(L(E/\mathbb{Q}, \chi, s)) = 1$ なる K がとれ Th. 1 を適用できる。

次に $\#Ш(E/K)$ の評価に進もう。簡単のため E は complex multiplication は持たないとし, 次のような素数 p の p-part を考えることにする。

Definition 素数 p が E に対して admissible であるとは, $p \neq 2$ かつ E の Tate module への作用 $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \operatorname{Aut}(T_p(E)) \cong GL_2(\mathbb{Z}_p)$ が全射であるということ。

Serre の定理により ほとんどすべての素数（有限個を除いて）は admissible である。また Mazur の定理により N_0 が square-free であれば $p \geqslant 11$ なる p は admissible である。

まず Gross Zagier の公式を思い出そう。

Th. (Gross Zagier) E, K をよの通りとすると

$$L'(E/K, 1) = V_\infty \cdot \hat{h}(y_K) / c^2 \cdot (\#\mathcal{O}_K^\times)^2 \sqrt{D}$$

ここに $\hat{h}$ は canonical height, $y_K \in E(K)$ は Heegner point (§3に後述), c は ω を Néron differential とし, $\varphi : X_0(N_0) \longrightarrow E$ による いまそだしが $\varphi^*(\omega) = c \sum a_n q^n \frac{dq}{q}$, $\sum a_n q^n$ は normalized new-form, となるような自然数。

この式から $L'(E/K, 1) \neq 0$ のとき Birch Swinnerton-Dyer 予想は次の型になる。

$$\#Ш(E/K) = (E(K) : \langle y_K \rangle)^2 / c^2 (\#\mathcal{O}_K^\times)^2 V_{bad}$$

ここに $\langle y_K \rangle$ は y_K の生成する $E(K)$ の部分群である。分母は一般に小さい数なのでこの式はほぼ $\#Ш(E/K) \fallingdotseq (E(K) : \langle y_K \rangle)^2$ と言っていると思ってよい。

Theorem 2. $L'(E/K, 1) \neq 0$ と仮定する。p を admissible な素数とし $y_K \in p^a E(K) \setminus p^{a+1} E(K)$ とする。$Ш(E/K)\{p\}$ を $Ш(E/K)$ の p-part (p のべきで消える元全体のなす部分群) とすると このとき $p^a \cdot Ш(E/K)\{p\} = 0$, $\#Ш(E/K)\{p\} \leqslant p^{2a}$ が成立する。

Remark 1. $L'(E/K,1) \neq 0$ とすると Gross Zagier の公式から y_K の位数は無限である。従って $y_K \in p^a E(K) \setminus p^{a+1} E(K)$ をみたすような自然数 a は必ず存在する。

Remark 2. $(E(K) : \langle y_K \rangle)$ が有限かどうかは最初はわからない。そこで a を定義するのにこのような書き方をしたのであるが、それは $\mathrm{ord}_p(\#(E(K) : \langle y_K \rangle)) = a$ のつもりである。特に Th. 2 の order についての主張は $\#(Ш(E/K)[p^\infty]) \mid (E(K) : \langle y_K \rangle)^2$ を導く。

Remark 3. admissible でない p についても $\#Ш(E/K)[p^\infty]$ についてのそうかし悪い評価なら出すことができる。(cf. [1])

§3. Heegner points のなす系

§2 の記号をそのまま使う。K の ideal $i \subset \mathcal{O}_K$ で $\mathcal{O}_K/i \simeq \mathbb{Z}/N_0\mathbb{Z}$ なるものを1つとる。$(n, N_0) = 1$ なる n に対して $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_K$, $i_n = i \cap \mathcal{O}_n$ とおく。$(\mathbb{C}/\mathcal{O}_n, \mathbb{C}/\mathcal{O}_n \to \mathbb{C}/i_n^{-1})$ は modular curve $X_0(N_0)$ の $\mathbb{C}$ 有理点を定めるが complex multiplication の理論によりこの点は conductor n の ring class field K_n 上に定義される。この点を x_n とおく。$x_n \in X_0(N_0)(K_n)$。$\varphi : X_0(N_0) \to E$ を parametrization として $y_n = \varphi(x_n)$ とおく。§2 の y_K は $N_{K_1/K}(y_1) = y_K$ によって定義される。ここに $N_{K_1/K} : E(K_1) \to E(K)$ は norm map。

Kolyvaginはすべてのnについてy_nを考えているが、定理の証明には特別なnだけを考えれば十分なので、ここでは次のようなnのみを考える。また簡単のため以下admissibleなpのp partを考えていくことにする。以下admissibleなpと自然数N（十分大きくとる）をfixする。

$S = \{\ell$：素数 $|$ $\ell \nmid Np$, $\mathrm{Gal}(K(E[p^N])/\mathbb{Q})$ の中でℓでのFrobenius置換 Frob_ℓ が複素共役のconjugacy classに等しい$\}$

とおく。ここに$K(E[p^N])$はKにEのp^N等分点をすべてつけ加えて得られる拡大である。以下nとしてはSのsquarefreeな積のみを考えることにする。（ただし1を含む。）

(y_n)はKolyvaginの用語によればEuler systemをなす。[1]ではEuler systemという概念がいくつかの公理をみたすものとして定義されているが、それはまだあまり整理されたものでなく、ただcyclotomic units, elliptic units, Gauss sum, Heegner pointsという4つの例をまとめて扱うことができる程度に抽象化したものように見える。ただKolyvaginはこのideaをもっとずっと一般化しようという考えは持っているようである。Euler systemの公理のうち最も重要なのはNormに関する性質である。(y_n)の場合，$N_{K_{n\ell}/K_n}(y_{n\ell}) = a_\ell \cdot y_n$，$a_\ell = \ell + 1 - \#E(\mathbb{F}_\ell)$ なる性質をみたす。（$n\ell$はSのsquarefreeな積と仮定している。）

n を S の元の squarefree な積とすると $\mathrm{Gal}(k_n/k_1) \simeq \prod_{l|n} \mathrm{Gal}(k_l/k_1)$, $\mathrm{Gal}(k_l/k_1)$ は位数 $l+1$ の巡回群である。$\mathrm{Gal}(k_l/k_1)$ の生成元 σ_l を1つとり,

$$D_l = \sum_{i=1}^{l} i\sigma_l^i \quad , \quad D_n = \prod_{l|n} D_l$$

とおく。S の定義から $D_n y_n \in (E(k_n)/p^N)^{\mathrm{Gal}(k_n/k_1)}$ を示すことができる。次の写像による $D_n y_n$ の像を $k(n)$ と書く。

$$\begin{array}{ccccc} (E(k_n)/p^N)^{\mathrm{Gal}(k_n/k_1)} & \overset{\partial}{\hookrightarrow} & H^1(k_n, E[p^N])^{\mathrm{Gal}(k_n/k_1)} & \underset{(*)}{\overset{\sim}{\leftarrow}} & H^1(k_1, E[p^N]) \\ \downarrow & & & & \downarrow \mathrm{Cor}_{k_1/k} \\ D_n y_n & \longmapsto & & & k(n) \in H^1(k, E[p^N]) \end{array}$$

ここに $E[p^N]$ は E の p^N 等分点のなす Galois module, ∂ は Kummer sequence $0 \to E[p^N] \to E \xrightarrow{p^N} E \to 0$ の boundary map, 自然な写像 $(*)$ は p についての仮定から同型。この元 $k(n)$ が市村氏の紹介の中の k_n と同じ役割を果たすのである。

v を K の素点とし、自然な写像による $k(n)$ の $H^1(k_v, E[p^N])$, ${}_{p^N}H^1(k_v, E)$ での像をそれぞれ $k(n)_v$, $\widetilde{k(n)}_v$ と書くことにする。

$$\begin{array}{ccccc} H^1(K, E[p^N]) & \longrightarrow & H^1(k_v, E[p^N]) & \longrightarrow & {}_{p^N}H^1(K, E) \\ k(n) & \longmapsto & k(n)_v & \longmapsto & \widetilde{k(n)}_v \end{array}$$

<u>Key Proposition</u> 1) $v \nmid n$ に対して $\widetilde{k(n)}_v = 0$

2) v を K の素点, $l|v$ (l: 素数), nl を S の元の squarefree な積とする。このとき任意の自然数 m に対して

$$\widetilde{k(nl)}_v \in p^m \cdot {}_{p^N}H^1(k_v, E) \iff k(n)_v \in p^m \cdot H^1(k_v, E[p^N])$$

もう1つ重要な命題を述べる。

Proposition. ε を $L(E/\mathbb{Q}, s)$ の関数等式の符号, $n = l_1 \cdots l_g$ とするとき $\kappa(n) \in H^1(K, E[p^N])^{(-1)^{g-1}\varepsilon}$。ここに $H^1(K, E[p^N])^{\mu}$ は ($\mu = \pm 1$) $H^1(K, E[p^N])$ の複素共役が μ 倍で act する部分。

このことから $n = l_1 \cdots l_g$ とすると

$$\widetilde{\kappa(nl)}_v \in {}_{p^N}H^1(K_v, E)^{(-1)^g\varepsilon}, \quad \kappa(n)_v \in H^1(K_v, E[p^N])^{(-1)^{g-1}\varepsilon}$$

一方 $l \in S$ から上の2つの群は共に位数 p^N の巡回群であることがわかる。位数 p^N の巡回群に対して ord_p を p で何回割れるかにより 0から N までの整数を対応させる写像とする。このとき Key Prop. 2) の述べるところは $\mathrm{ord}_p(\widetilde{\kappa(nl)}_v) = \mathrm{ord}_p(\kappa(n)_v)$ である。

§4. Galois cohomology についての準備.

円分体 K の類数(a p-part)が予想される値で押さえられるということを Kolyvagin は証明したが (cf. 市村氏の紹介), その idea は完全系列

$$K^\times/p^N \longrightarrow \bigoplus \mathbb{Z}/p^N \longrightarrow \mathrm{Pic}\,\mathcal{O}_K/p^N \longrightarrow 0 \quad (\mathrm{Pic}\,\mathcal{O}_K : \text{ideal 類群})$$

を使い, $K^\times/p^N$ の中に定義された $\kappa(n)$ というものが $\bigoplus \mathbb{Z}/p^N$ の大部分を消してしまう ということからできていた。ここでは上の完全系列の役割を果たす完全系列を作りたい。下, K, p, S などは §3 の通りとする。

まず自然数 m に対して Selmer 群をいつものように

$$Sel(E/k)[m] := \ker\left(H^1(k, E[m]) \longrightarrow \prod_{all\ v} H^1(k, E)\right)$$

と定義する。定義から次の完全系列を得る。

$$(4.1) \qquad 0 \longrightarrow E(k)/m \longrightarrow Sel(E/k)[m] \longrightarrow {}_m Ш(E/k) \longrightarrow 0$$

Remark. Galois cohomology の一般論により $Sel(E/k)[m]$ は有限群である。従って weak Mordell Weil の定理と ${}_m Ш(E/k)$ の有限性が出る。

次の完全系列から成る図式を考える。

$$\begin{array}{ccccc}
 & & 0 & & 0 \\
 & & \uparrow & & \uparrow \\
 & \nearrow & \bigoplus_{p^N} H^1(k_v, E) & \longrightarrow & Sel(E/k)[p^N]^\vee \longrightarrow 0 \\
 & & \uparrow & & \uparrow \\
H^1(k, E[p^N]) & \longrightarrow & Ш\, H^1(k_v, E[p^N]) & \longrightarrow & H^1(k, E[p^N])^\vee \longrightarrow 0 \\
 & & \uparrow & & \\
 & & \prod E(k_v)/p^N & & \\
 & & \uparrow & & \\
 & & 0 & &
\end{array}$$

ここに横の完全列は Tate-Poitou の exact sequence, p についての仮定から最後が全射となる。たては Kummer sequence から得られる完全系列である。上の図式から次の完全列を得る。

$$(4.2) \qquad H^1(k, E[p^N]) \longrightarrow \bigoplus_{all\ v} {}_{p^N} H^1(k_v, E) \longrightarrow Sel(E/k)[p^N]^\vee \longrightarrow 0$$

これがこの§の最初に書いた ideal 類群の完全列と同じ役割を果たす完全列である。

Remark p が admissible でないとき、(4.2) の2つめの写像は全射にはならない。しかしその余核の位数を N によらぬ数で押

さえることができる。

§5. 定理の証明

$y_K \in p^a E(K) \setminus p^{a+1} E(K)$ とする。$y_K = p^a \cdot y'_K$ $y'_K \in E(K)$ と書き、(4.1) により y'_K の $Sel(E/K)[p^N]$ の中で生成する部分群を $\langle y'_K \rangle$ と書く。ここの目標は次を証明することである。

Theorem 3. $A = Sel(E/K)[p^N] / \langle y'_K \rangle$ とおくと

(1) $p^a \cdot A = 0$

(2) $\# A \leqq p^{2a}$

まずこの定理から Th.1 のほとんどと Th.2 が出ることを示そう。$E(K)$ は有限生成 abel 群だから、ほとんどの p について $a=0$ である。このような p に対して (1) は $Sel(E/K)[p^N] = \langle y_K \rangle$ を導く。従って (4.1) により $E(K)/p$ は y_K で生成され、$\operatorname{rank} E(K) = 1$。次に (2) はこのことより $\# Ш(E/K)[p^\infty] \leqq p^{2a}$ を導く。なお admissible でない p についても、もっと悪い評価だが $\# A$ を N によらぬ数で押さえることができる。かくて $Ш(E/K)$ の有限性が出るのである。

Th.3 の証明の概略に進もう。ε を $L(E/\mathbb{Q}, s)$ の関数等式の符号とし、(4.2) の ε-part をとった

$$(4.2)^\varepsilon \quad H^1(K, E[p^N])^\varepsilon \xrightarrow{\psi_1} \bigoplus_{p^N} H^1(K_v, E)^\varepsilon \xrightarrow{\psi_2} (Sel(E/K)[p^N])^{V\varepsilon} \to 0$$

を考える。$x_1 \in (A^V)^\varepsilon$ をとり $(Sel(E/K)[p^N])^{V\varepsilon}$ の元と見る。このとき Čebotarev density theorem により次のような K の素点 v_1

をとることができる。

1) v_1 の下にある素数を ℓ_1 とする ($(\ell_1)=v_1\cap\mathbb{Z}$) と $\ell_1\in S$

2) $\psi_2(0,\cdots,0,\underset{(v_1)}{u_1},0,0\cdots)=x_1$. ここに $(0,\cdots 0,u_1,0,0\cdots)$ は v_1 のところに u_1 があり他はすべて 0 の $\bigoplus_{p^N} H^1(K_v,E)^\varepsilon$ の元。1) から ${}_{p^N}H^1(K_{v_1},E)^\varepsilon$ は位数 p^N の巡回群となるが u_1 はこの群の生成元。

3) $(y_k)_{v_1}\notin p^{a+1}E(K_{v_1})$

このように v_1, ℓ_1 をとるとき Key Prop. から $\psi_1(k|\ell_1))=(0\cdots 0,\underset{(v_1)}{c_1},0,0\cdots)$ ここに $\mathrm{ord}_p(c_1)=\mathrm{ord}_p(\widetilde{k|\ell_1)}_{v_1})=\mathrm{ord}_p(k|1)_v)$ $=\mathrm{ord}_p((y_k)_v)=a$ (ord_p は位数 p^N の巡回群の元に対し、p で何回割れるかにより 0 から N までの整数を対応させる写像) 従って $(4.2)^\varepsilon$ により $p^a\cdot x_1=0$。特に $p^aA^\varepsilon=0$ である。

次に $k(\ell_1)\in p^bH^1(K,E[p^N])$ となるような最大の b をとる。(もちろん b は x_1, ℓ_1 による。) この b を使えば $p^{a-b}x_1=0$ が示せる。$-\varepsilon$ part についても次の完全系列を考える。

$(4.2)^{-\varepsilon}$. $H^1(K,E[p^N])^{-\varepsilon}\xrightarrow{\psi_1}\bigoplus_{p^N}H^1(K_v,E)^{-\varepsilon}\xrightarrow{\psi_2}(Sel(E/K)[p^N])^{V-\varepsilon}\to 0$

$x_1'\in(A^V)^{-\varepsilon}$ をとると Čebotarev density により次のような v_1' をとることができる.

1) v_1' の下にある素数を ℓ_1' とすると $\ell_1'\in S$

2) $\psi_2(0,\cdots 0,\underset{(v_1')}{u_1'},0,0\cdots)=x_1'$ ここに u_1' は ${}_{p^N}H^1(K_{v_1'},E)^{-\varepsilon}\simeq\mathbb{Z}/p^N$ の生成元 (i.e. $\mathrm{ord}_p u_1'=0$)

3) $k(l_1)_{v_1'} \notin p^{b+1} H^1(K_{v_1'}, E[p^N])$ (i.e. $\mathrm{ord}_p(k(l_1)_{v_1'}) = b$)

4) $k(l_1') = 0$

このとき $k(l_1 l_1')$ を考えると §3 の Key Prop. から $\mathrm{ord}_p(\widetilde{k(l_1 l_1')}_{v_1}) = \mathrm{ord}_p(k(l_1')_{v_1}) = 0$, 従って $\psi_1(k(l_1 l_1')) = (0, \cdots 0, \underset{(v_1')}{\widetilde{k(l_1 l_1')}_{v_1'}}, 0, 0 \cdots)$. さらに Key Prop. により $\mathrm{ord}_p(\widetilde{k(l_1 l_1')}_{v_1'}) = \mathrm{ord}_p(k(l_1)_{v_1'}) = b$. 完全列 $(\sharp 2)^{-\varepsilon}$ を考えるとこれは $p^b x_1' = 0$ を導く。特に $p^b \cdot A^{-\varepsilon} = 0$ である。$b \leqq a$ であったから ε-part とあわせて Th. 3 (1) が示された。(1) が示されたことにより $Ш(E/k)[p^\infty]$ は有限群で、$N \geqq a$ にとれば $A \simeq Ш(E/k)[p^N]$ であることに注意しておく。

(2) を示すには上の操作をくり返すのである。$A^\vee$ の構造は $(A^\vee)^\varepsilon \simeq A_1 \oplus \cdots \oplus A_r$, $A_i \simeq (\mathbb{Z}/p^{n_i})^{\oplus 2}$, $(A^\vee)^{-\varepsilon} \simeq A_1' \oplus \cdots \oplus A_r'$, $A_r' \simeq (\mathbb{Z}/p^{n_i'})^{\oplus 2}$ となっており、$x_1, \cdots x_r$ を $A_1, \cdots A_r$ の元で位数が $p^{n_1}, \cdots, p^{n_r}$ のもの、$x_1', \cdots, x_r'$ を $A_1', \cdots, A_r'$ の元で位数が $p^{n_1'}, \cdots p^{n_r'}$ のもの として、上の操作を続ける。すなわち x_1, x_1' に対して上のように l_1, l_1' をとる。さらに $k(l_1 l_1') \in p^c \cdot H^1(K, E[p^N])$ となるような最大の c をとる。このとき $p^{b-c} x_1' = 0$。さらに上と同様にして l_2 をうまくとり、$k(l_1 l_1' l_2)$ を考えることにより $p^c \cdot x_2 = 0$ を示すことができる。これをくり返せば、$p^{a-b} x_1 = 0$, $p^{b-c} x_1' = 0$, $p^{c-d} x_2 = 0$, $p^{d-e} x_2' = 0$, $\cdots$, 従って $a - b \geqq n_1$, $b - c \geqq n_1'$, $c - d \geqq n_2 \cdots$。故に $\sum n_i + \sum n_i' \leqq a$。より $\# A \leqq p^{2a}$ となる。

References

[1] V. A. Kolyvagin, Euler systems (preprint)

[2] V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves, Math. USSR Izvestija Vol 32 (1989) (英訳)

[3] K. Rubin, The Main Conjecture, appendix to Cyclotomic fields I and II by S Lang (second edition) GTM 121

[4] K. Rubin, Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. math 89 (1987)

[5] B. Gross, Kolyvagin's work on modular elliptic curves (preprint)

[6] D. Husemöller, Elliptic curves GTM 111

[7] J. H. Silverman, The arithmetic of elliptic curves GTM 106

[8] F. Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. 128 (1988)